Claims

We claim:

1. A method for use in a device associated with a first party for decrypting a ciphertext according to a Cramer-Shoup based encryption scheme, the method comprising the steps of:

obtaining the ciphertext in the first party device; and

generating in the first party device a plaintext corresponding to the ciphertext based on assistance from a device associated with a second party, the plaintext representing a result of the decryption according to the Cramer-Shoup based encryption scheme.

2. The method of claim 1, wherein the generating step further comprises an exchange of information between the first party device and the second party device whereby at least a portion of the information is encrypted using an encryption technique such that one party encrypts information using its own public key and another party can not read the information but can use the information to perform an operation.

3. The method of claim 1, wherein the generating step further comprises an exchange of information between the first party device and the second party device whereby at least a portion of the information is encrypted using an encryption technique having a homomorphic property.

4. The method of claim 1, wherein the generating step further comprises:

generating a share of a random secret;

generating information representing encryptions of a form of the random secret, a share of a private key, and the ciphertext;

transmitting at least the encrypted information to the second party device; and

computing the plaintext based at least on the share of the random secret, the share of the private key, the ciphertext, and the data received from the second party device.

5. The method of claim 1, wherein the first party device and the second party device additively share components of a private key.

6. The method of claim 1, wherein the generating step further comprises generation and exchange of proofs between the first party device and the second party device that serve to verify operations performed by each party.

7. The method of claim 6, wherein the proofs are consistency proofs based on three-move Σ-protocols.

8. A method for use in a device associated with a first party for assisting in decrypting a ciphertext according to a Cramer-Shoup based encryption scheme, the method comprising the steps of:

receiving a request generated in and transmitted by a second party device for the partial assistance of the first party device in decrypting the ciphertext according to the Cramer-Shoup based encryption scheme; and

generating results in the first party device based on the partial assistance provided thereby for use in the second party device to complete decryption of the ciphertext.

9. Apparatus for use in a device associated with a first party for decrypting a ciphertext according to a Cramer-Shoup based encryption scheme, the apparatus comprising:

a memory; and

at least one processor coupled to the memory and operative to: (i) obtain the ciphertext in the first party device; and (ii) generate in the first party device a plaintext corresponding to the ciphertext based on assistance from a device associated with a second party, the plaintext representing a result of the decryption according to the Cramer-Shoup based encryption scheme.

10. The apparatus of claim 9, wherein the generating operation further comprises an exchange of information between the first party device and the second party device whereby at least a portion of the information is encrypted using an encryption technique such that one party encrypts information using its own public key and another party can not read the information but can use the information to perform an operation.

11. The apparatus of claim 9, wherein the generating operation further comprises an exchange of information between the first party device and the second party device whereby at least a portion of the information is encrypted using an encryption technique having a homomorphic property.

12. The apparatus of claim 9, wherein the generating operation further comprises: (i) generating a share of a random secret; (ii) generating information representing encryptions of a form of the random secret, a share of a private key, and the ciphertext; (iii) transmitting at least the encrypted information to the second party device; and (iv) computing the plaintext based at least on the share of the random secret, the share of the private key, the ciphertext, and the data received from the second party device.

13. The apparatus of claim 9, wherein the first party device and the second party device additively share components of a private key.

14. The apparatus of claim 9, wherein the generating operation further comprises generation and exchange of proofs between the first party device and the second party device that serve to verify operations performed by each party.

15. The apparatus of claim 14, wherein the proofs are consistency proofs based on three-move Σ-protocols.

16. Apparatus for use in a device associated with a first party for assisting in decrypting a ciphertext according to a Cramer-Shoup based encryption scheme, the apparatus comprising:

a memory; and

at least one processor coupled to the memory and operative to: (i) receive a request generated in and transmitted by a second party device for the partial assistance of the first party device in decrypting the ciphertext according to the Cramer-Shoup based encryption scheme; and (ii) generate results in the first party device based on the partial assistance provided thereby for use in the second party device to complete decryption of the ciphertext.